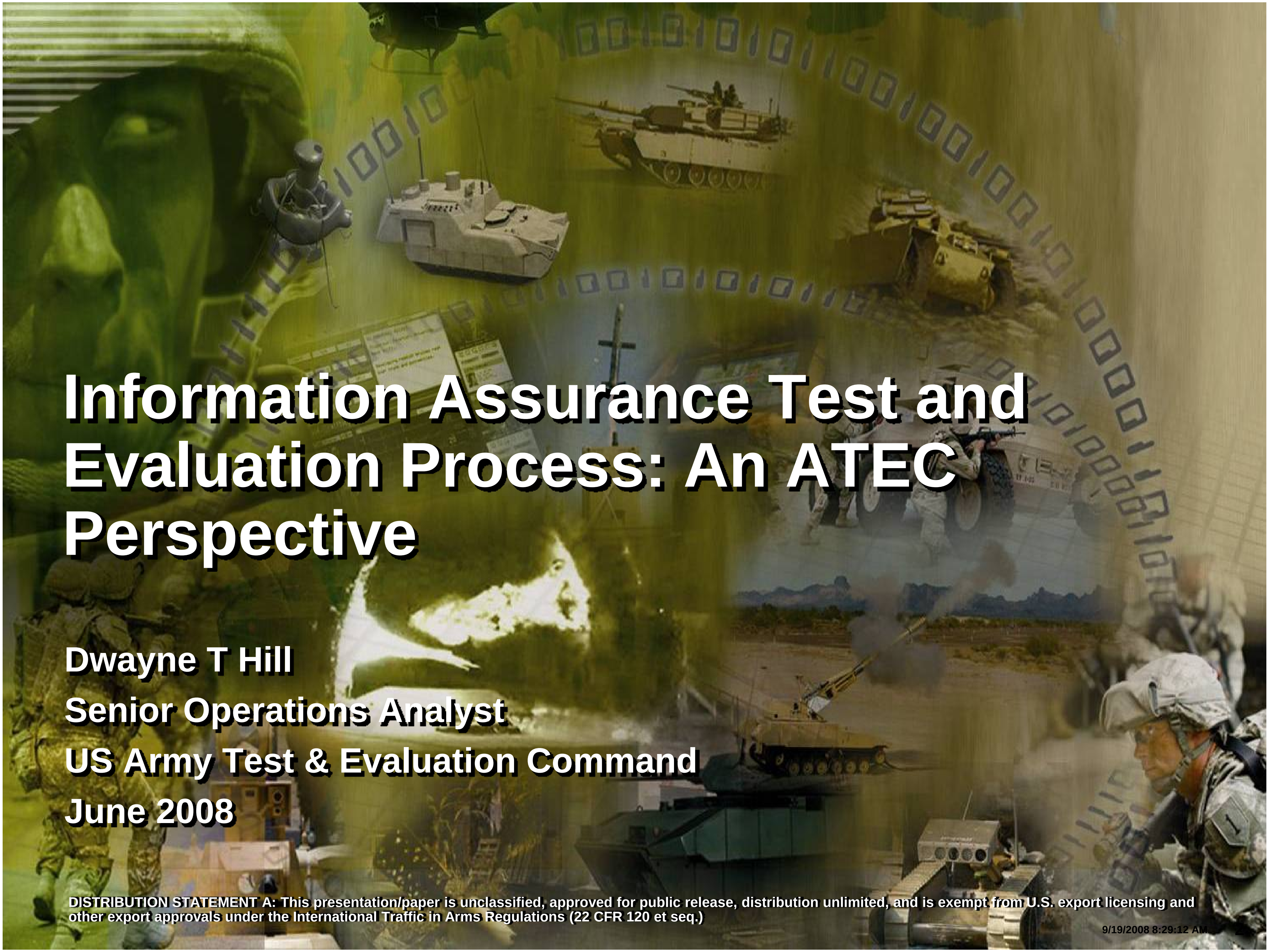


Information Assurance Test and Evaluation Process: An ATEC Perspective

Dwayne T Hill

Senior Operations Analyst

US Army Test & Evaluation Command

June 2008

DISTRIBUTION STATEMENT A: This presentation/paper is unclassified, approved for public release, distribution unlimited, and is exempt from U.S. export licensing and other export approvals under the International Traffic in Arms Regulations (22 CFR 120 et seq.)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **01 JUN 2008**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Information Assurance Test and Evaluation Process: An ATEC Perspective**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army Test & Evaluation Command CSTE-TT-MD**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202527. Military Operations Research Society Symposium (76th) Held in New London, Connecticut on June 10-12, 2008, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**13**	

Agenda

- Purpose
- Information Assurance Policy
- Net-Readiness
- DIACAP – The Army Way
- DOT&E Policy
- Testing for Information Assurance Methodology
- IA Issues

Purpose

- Provide information about the current ATEC methodology for conducting Information Assurance (IA) assessments
- Describe challenges to correctly characterizing system IA capabilities

Information Assurance Policies

Public Law 107-347 – Agencies identify & provide information security protection

DoDD 8500.1 – IA requirements included in all aspects of DoD information systems

DoDI 8500.2 – Provides baseline IA controls for DoD information systems

DoD CIO Memorandum, DIACAP – Requires DoD to certify and accredit information systems

CJCSI 6212.01 – Requires Joint IT and NSS to be IA compliant

AR 25-1 – Establishes the Army IA program for infrastructure, networks and systems

AR 25-2 – Implementation guidance for the Army IA program

DA CIO/G-6 Memorandum – Army implementation of DIACAP

Protect, Detect, React & Restore

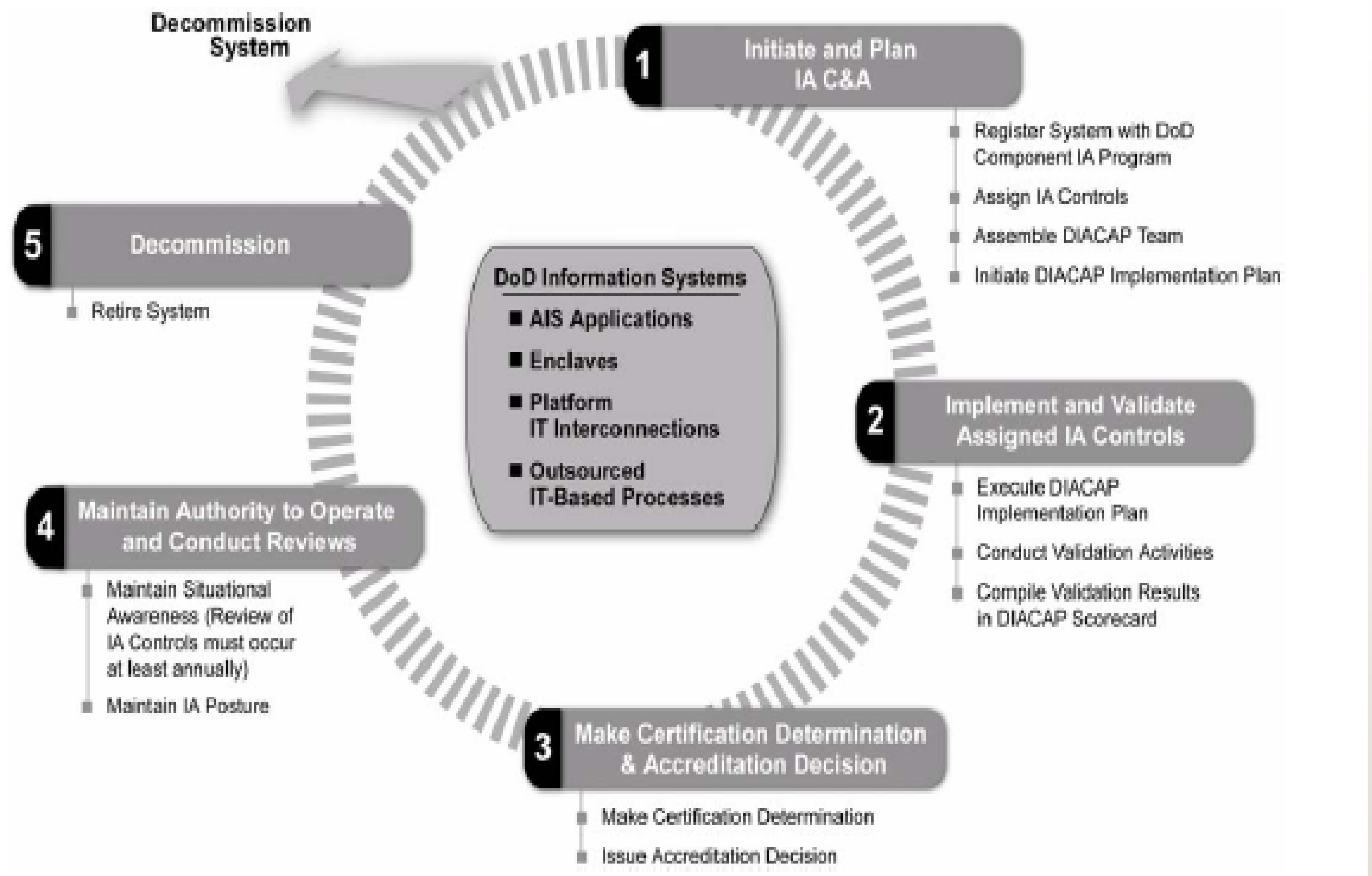
Net-Readiness

- NR-KPP consists of **verifiable performance measures and metrics** used **to assess** … **information assurance**, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange
- Four NR-KPP elements include: compliance with …, and verification of compliance with DOD information assurance requirements
- IA policies and processes **apply to the entire lifecycle** of IT and NSS
- Threshold criteria - Information assurance requirements including **availability, integrity, authentication, confidentiality, and nonrepudiation**, and issuance of an **IATO** by the DAA
- Objective criteria - Information assurance requirements including availability, integrity, authentication, confidentiality, and nonrepudiation, and issuance of an **ATO** by the DAA

DIACAP – Why Transition?

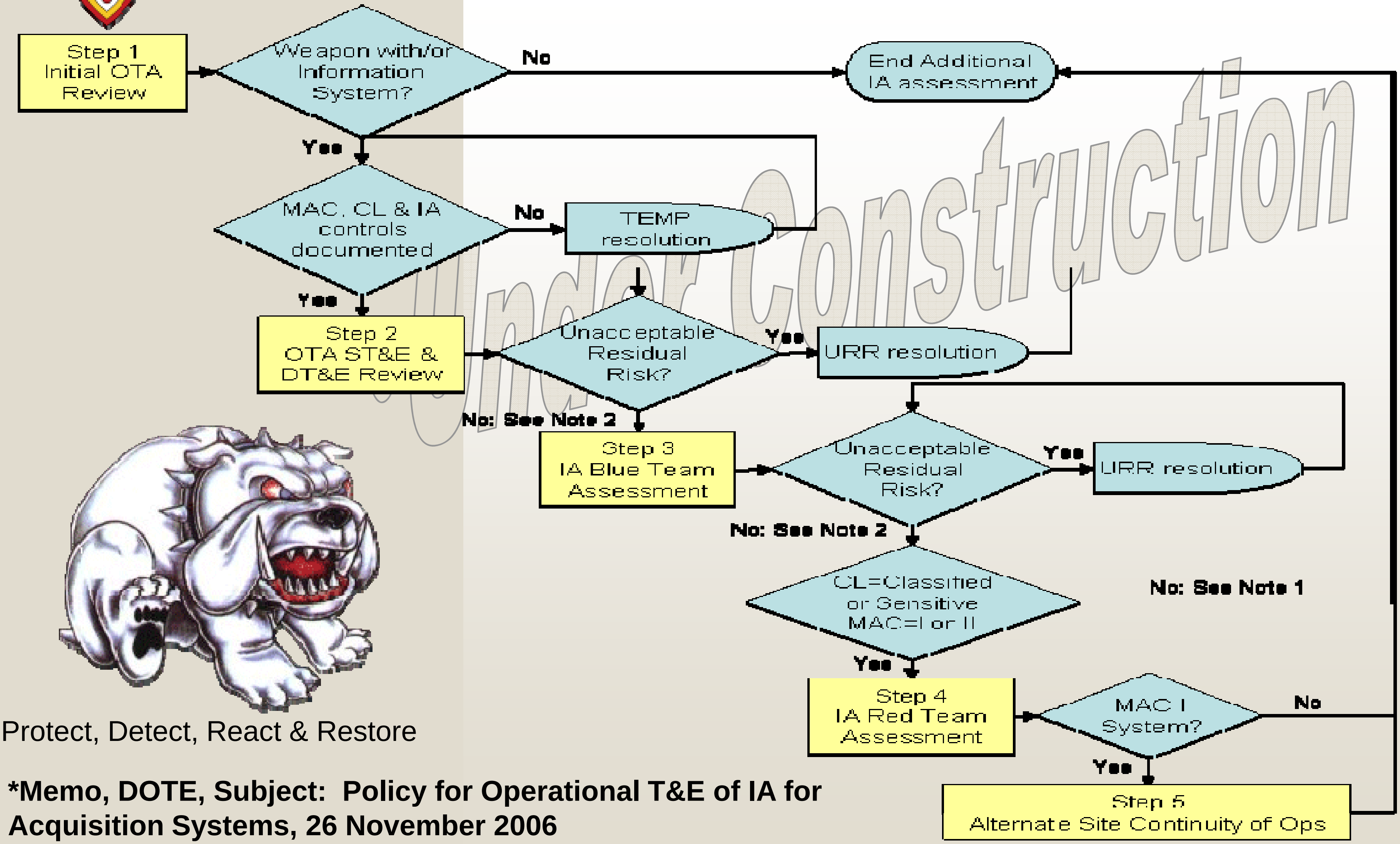
https://diacap.iaportal.navy.mil

- DITSCAP & Army C/A processes written for stand alone or stove pipe systems
- DODI 8500.2 IA controls not considered
- DAA delegated to the lowest level limits "Big Picture" consideration
- Too many CAs limits consistent assessments
- No qualification requirements for ACAs
- IS deployed with no easily identifiable responsible government owner


Decommission System
1 Initiate and Plan IA C&A
Register System with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Initiate DIACAP Implementation Plan
2 Implement and Validate Assigned IA Controls
Execute DIACAP Implementation Plan
Conduct Validation Activities
Compile Validation Results in DIACAP Scorecard
3 Make Certification Determination & Accreditation Decision
Make Certification Determination
Issue Accreditation Decision
4 Maintain Authority to Operate and Conduct Reviews
Maintain Situational Awareness (Review of IA Controls must occur at least annually)
Maintain IA Posture
5 Decommission
Retire System
DoD Information Systems
AIS Applications
Enclaves
Platform IT Interconnections
Outsourced IT-Based Processes

DIACAP does not ensure IA; only shows how well system has implemented baseline controls

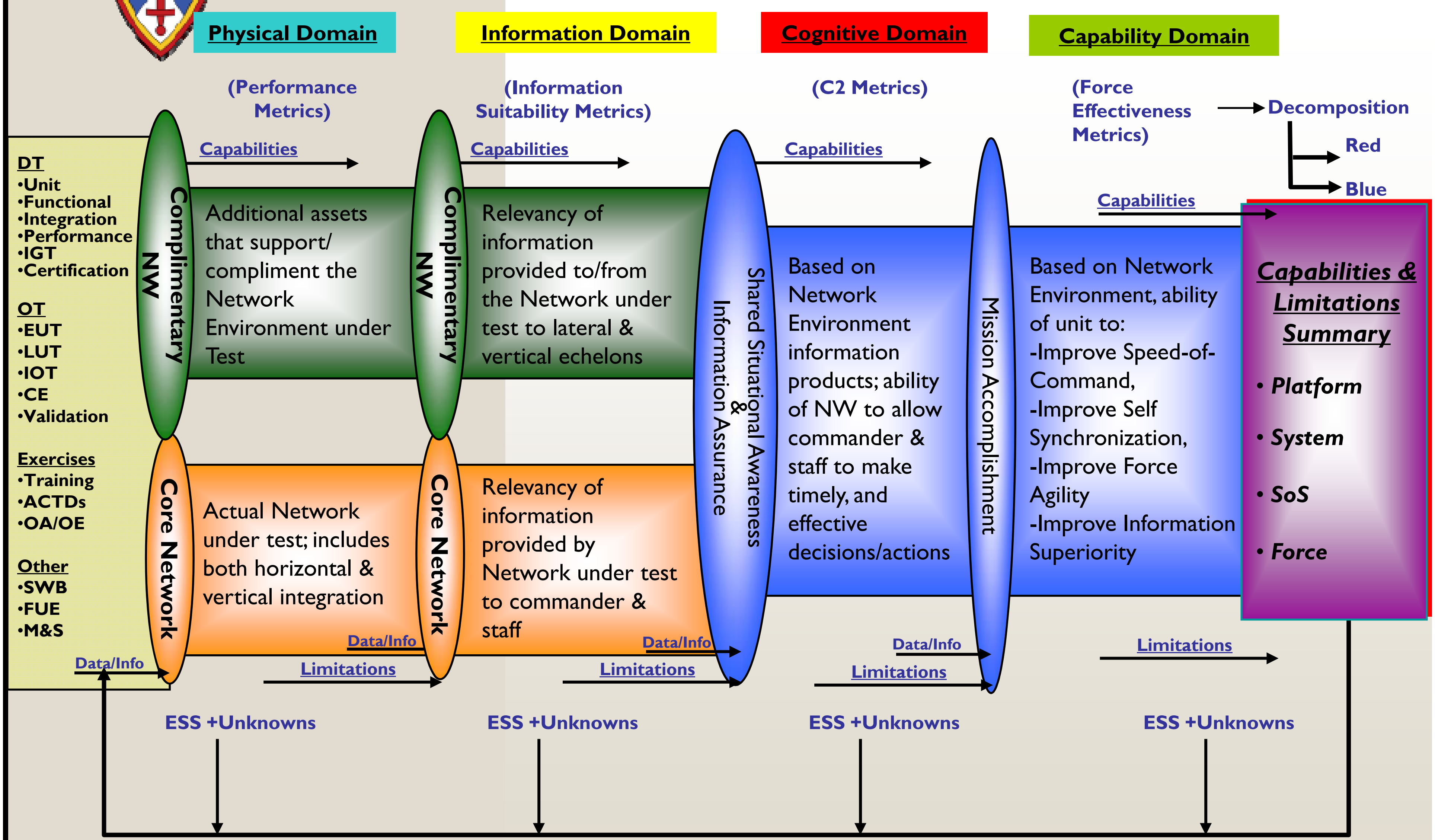
DOT&E Policy



Protect, Detect, React & Restore

***Memo, DOTE, Subject: Policy for Operational T&E of IA for Acquisition Systems, 26 November 2006**

ATEC IA Methodology



Physical Domain

(Performance Metrics)

Information Domain

(Information Suitability Metrics)

Cognitive Domain

(C2 Metrics)

Capability Domain

(Force Effectiveness Metrics)

→ Decomposition

→ Red

→ Blue

DT
- Unit
- Functional
- Integration
- Performance
- IGT
- Certification

OT
- EUT
- LUT
- IOT
- CE
- Validation

Exercises
- Training
- ACTDs
- OA/OE

Other
- SWB
- FUE
- M&S

Complimentary NW

Additional assets that support/ compliment the Network Environment under Test

Complimentary NW

Relevancy of information provided to/from the Network under test to lateral & vertical echelons

Core Network

Actual Network under test; includes both horizontal & vertical integration

Core Network

Relevancy of information provided by Network under test to commander & staff

Shared Situational Awareness & Information Assurance

Based on Network Environment information products; ability of NW to allow commander & staff to make timely, and effective decisions/actions

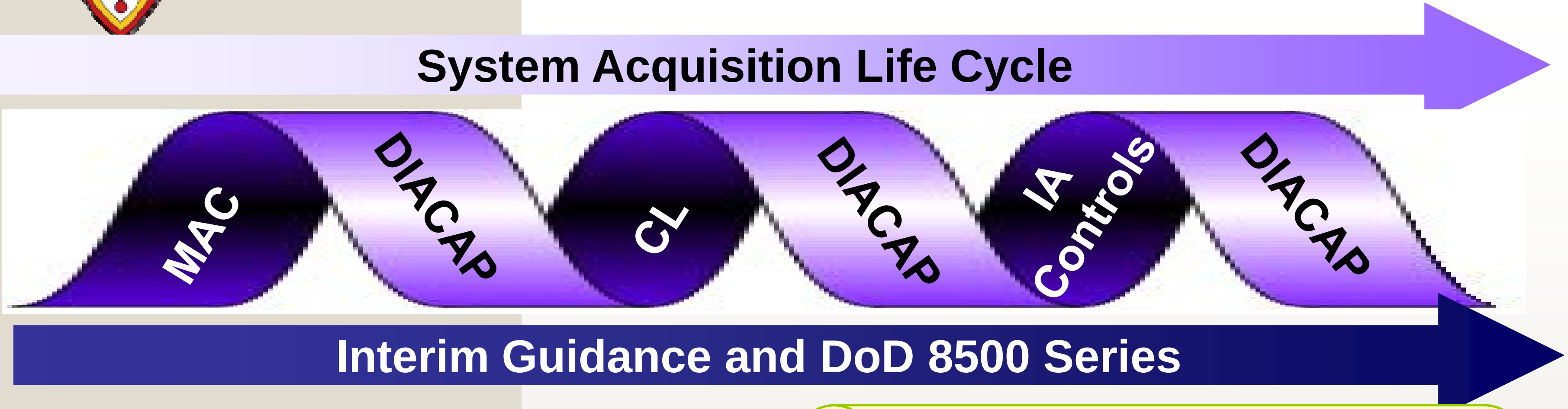
Mission Accomplishment

Based on Network Environment, ability of unit to:
-Improve Speed-of-Command,
-Improve Self Synchronization,
-Improve Force Agility
-Improve Information Superiority

Capabilities & Limitations Summary
- ***Platform***
- ***System***
- ***SoS***
- ***Force***

IGT - Independent Government Test; EUT – Early User Test; LUT – Limited User Test; IOT – Initial Operational Test; CE – Continuous Evaluation; ACTD – Advanced Concept Technology Demonstration; OA/OE – Operational Assessment/Operational Evaluation; SWB – Software Blocking; FUE – First Unit Equipped; M&S – Modeling and Simulation; ESS – Effectiveness, Suitability, Survivability; NW – Network; C2 – Command and Control; FoS – Family of Systems; SoS – System of Systems

ATEC IA Methodology



System Acquisition Life Cycle

Interim Guidance and DoD 8500 Series

ATEC ensures PM documents IA plans and results; ATEC observes PM IA events to understand system C&L, how to test, compliance and readiness for OT

For DIACAP, PM responsible for conducting susceptibility analysis (laboratory/DT) not subject to AR 380-53 - PM will not portray Threat IO

IA OT Entrance Criteria

☑ **MAC and CL documented**

☑ **IA controls implemented**

☑ **DIACAP compliance review**

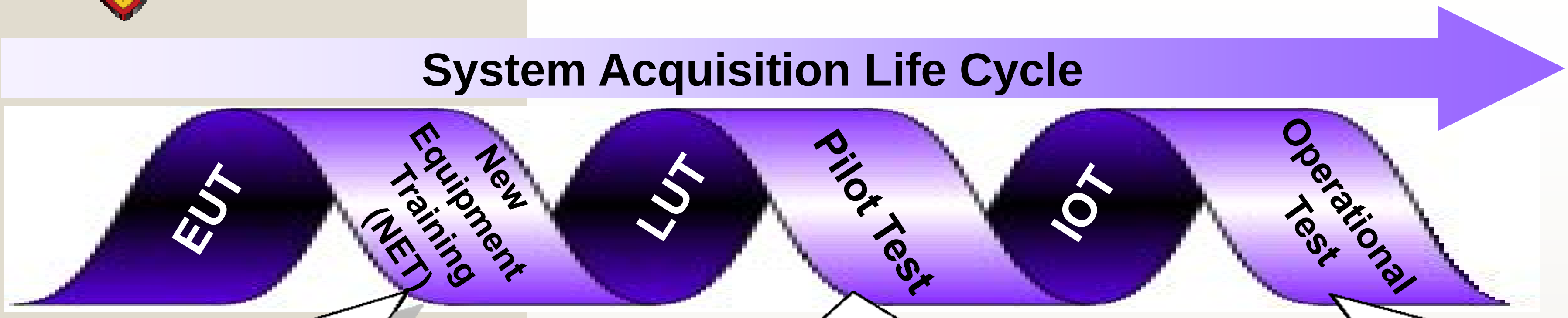
☑ **DAA approved SSAA (DITSCAP) or DIACAP POA&M, DIP**

☑ **ATO/IATO (before OT)**

☑ J-6 I&S Certification

☑ Other CJCSI 6212.01 compliance requirements met. (i.e. E3, HERO, SAASM, etc.)

ATEC IA Methodology



Training Assessment

- Participates in PM training and provides feedback on the quality of the Information Assurance training.

Susceptibility Assessment

- Conducts susceptibility testing

Data Collection

- Analyzes susceptibility data and assists in determining required fixes prior to OT start

Threat IO/Vulnerability Assessment

- Conducts "comm" checks

Susceptibility Assessment

- Continues to conduct susceptibility testing, if needed

Data Collection

- Observes Threat IO/penetration testing impacts on user and collects data

Threat IO (if IOT/FOC event)

- Conducts Threat IO activities (requires Threat commander and validated threat)

Vulnerability (other OT event)

- Conducts penetration testing

Begin planning and coordination early

IA Issues

- Metrics for determining IA capabilities:
  - ❑ Protect - How well does the enterprise, SoS, system defeat attacks / compromises?
  - ❑ Detect - How well does the enterprise, SoS, system detect and alert users of attacks / compromises?
  - ❑ React - How well does the enterprise, SoS, system react to attacks / compromises?
    - ▪ Was the response sufficient?
  - ❑ Restore - How well does the enterprise, SoS, system restore information / systems to per-attack / compromise status?

IA Issues

- Methodology for determining the correct balance between information assurance and interoperability
- Are the current IA baseline controls sufficient?
- Best use of M&S
- What is the best way to T&E an enterprise / federation, system-of-system?

Contacts

Melanie Miller
CSTE-TT-MD
(410) 278-1489
Melanie.L.Miller@us.army.mil

Dwayne T Hill
CSTE-TT-MD
(703) 681-2749
Dwayne.Thomas.Hill@us.army.mil